ADVISORY NUMBER:
SA2016-067

DATE(S) ISSUED:
04/29/2016

SUBJECT:
Multiple Vulnerabilities in Apache Struts Could Allow for Remote Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered for Apache Software Foundation Struts version 2. Apache Struts is an open source framework used for building Java web applications. Successful exploitation of these vulnerabilities could allow for remote code execution. Depending on the privileges associated with the application, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploitation could result in a denial-of-service condition.

THREAT INTELLIGENCE:
There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:
- Struts 2.0.0 - Struts Struts 2.3.28 (except 2.3.20.3, 2.3.24.3, and 2.3.28.1)

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: N/A

TECHNICAL SUMMARY:
Multiple vulnerabilities have been discovered in Apache Struts version 2, which could allow for remote code execution. Failed exploitation could cause a Denial of Service (DoS) condition. One vulnerability is caused when 'XSLTResult' does not properly sanitize data supplied by a user; resulting in a stylesheets location being passed as a request parameter, potentially allowing for the injection of remote code. XSLTResult uses EXtensible Stylesheet Language (XSLT), to transform an action object to EXtensible Markup Language (XML) and is installed by default in Struts version 2. The second vulnerability exists in the 'method: prefix' that could allow for remote code execution when Dynamic Method Invocation is enabled. Dynamic Method Invocation is enabled by default in Struts version 2.

Successful exploitation of these vulnerabilities could allow for remote code execution. Depending on the privileges associated with the application, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploitation could result in a denial-of-service condition.

RECOMMENDATIONS:
We recommend the following actions be taken:
- Upgrade to one of the non-impacted versions of Adobe Struts, either 2.3.20.3, 2.3.24.3 or 2.3.28.1, or follow the mitigation identified in the referenced Apache resources below.

- Verify no unauthorized system modifications have occurred on system before applying the patch.
- Frequently validate type and content of uploaded data.
- As a workaround, implement your own XSLTResult based on code of the recommended versions.

REFERENCES:

Apache:
https://struts.apache.org/docs/s2-031.html
https://struts.apache.org/docs/s2-032.html

CVE:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3082
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3081